Amendments to the Claims:

This listing of the claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method for securely providing information comprising the steps of:

(a) at a storage sever, receiving from the client information identifying an encrypted personal security device;

(b) in response to receiving said information identifying a personal security device, sending from the storage server to the client ~~providing~~ said identified encrypted personal security device;

(c) at an authentication server, receiving authentication information from the client; and

(d) responsive to said authentication information, sending from a key server to the client ~~providing~~ decryption information for said personal security device ~~responsive to said authentication information~~.

a'

2. (Canceled)

3. (Currently Amended) The method of claim ~~1~~ 54, wherein ~~step (a) comprises receiving information identifying an encrypted personal security device, the personal security device comprising~~ the encrypted container contains information necessary to make a secure network connection between a network client and a network server.

4. (Currently Amended) The method of claim ~~1~~ 54, wherein ~~step (a) comprises receiving information identifying an encrypted personal security device, the personal security device comprising~~ the encrypted container contains information necessary to make a secure virtual private network connection.

5. (Currently Amended) The method of claim ~~1~~ 54, wherein ~~further comprising the step of~~ authenticating involves validating said authentication information.

6. (Canceled)

7. (Cancelled)

8. (Cancelled)

9. (Cancelled)

10. (Currently Amended) The method of claim ~~1~~ 54, wherein ~~step (c) comprises receiving time dependent~~ the received authentication information includes a time-based authentication code ~~information~~.

11. (Currently Amended) A method implemented by a client for accessing secure information comprising the steps of:

(a) receiving from a storage server an encrypted personal security device;

(b) receiving from a key server decryption information for said personal security device; and

(c) decrypting said personal security device.

12. (Cancelled)

13. (Currently Amended) The method of claim ~~11~~ 70, wherein ~~receiving step (a) comprises receiving an~~ the encrypted container contains ~~personal security device comprising~~ information necessary to make a secure network connection between a network client and a network server.

14. (Currently Amended) The method of claim ~~11~~ 70, wherein ~~receiving step (a) comprises receiving an~~ the encrypted container contains ~~personal security device comprising~~ information necessary to make a secure virtual private network connection.

15. (Cancelled)

16. (Cancelled)

17. (Currently Amended) The method of claim ~~11~~ 70, wherein receiving the encrypted container involves receiving a smartcard that contains the encrypted container stored thereon ~~further comprising the step of storing said personal security device on a smartcard~~.

18. (Currently Amended) The method of claim ~~11~~ 70, further comprising ~~the step of~~ storing the received key ~~said decryption information~~ in a volatile memory ~~element~~.

19. (Canceled)
20. (Canceled)
21. (Canceled)
22. (Canceled)
23. (Canceled)
24. (Canceled)
25. (Canceled)
26. (Canceled)
27. (Canceled)
28. (Canceled)
29. (Canceled)
30. (Canceled)
31. (Canceled)
32. (Canceled)
33. (Canceled)
34. (Canceled)
35. (Canceled)
36. (Canceled)
37. (Canceled)
38. (Canceled)
39. (Canceled)
40. (Canceled)

41. (Canceled)

42. (Canceled)

43. (Canceled)

44. (Canceled)

45. (Canceled)

46. (Canceled)

47. (Canceled)

48. (Canceled)

49. (Canceled)

50. (Canceled)

51. (Canceled)

52. (New) The method of claim 1, further comprising implementing the storage server and the authentication server on the same computer.

a'

53. (New) The method of claim 1, further comprising implementing the authentication server and the key server on the same computer.

54. (New) A method for enabling a client to access secure information contained in an encrypted container, said method comprising:

at an authentication server, receiving from the client a key query that includes authentication information;

at the authentication server, authenticating the client based on the received authentication information; and

as a consequence of authenticating the client, sending a key from a key server to the client, said key for decrypting the identified encrypted container to access the secure information.

55. (New) The method of claim 54, wherein the key query identifyies the encrypted container

56. (New) The method of claim 54, further comprising:

at a storage sever, receiving from the client a request identifying the encrypted container containing secure information; and

in response to receiving said request, sending the identified encrypted container from the storage server to the client.

57. (New) The method of claim 54, wherein authenticating the client involves:

in response to receiving the key query, sending the client an authentication challenge; and

receiving at the authentication server a response from the client to the authentication challenge, said response including said authentication information.

58. (New) The method of claim 54, further comprising implementing the storage server and the authentication server on the same computer.

59. (New) The method of claim 54, further comprising implementing the authentication server and the key server on the same computer.

60. (New) The method of claim 54, wherein the encrypted container contains a cryptrographic key.

61. (New) The method of claim 54, wherein the encrypted container contains a password.

62 (New) The method of claim 54, wherein the encrypted container contains private or secret information selected from a group consisting of a medical record, contact information, a personal identification number, biometric information, a transaction record, and a map revealing a location of a resource.

63. (New) The method of claim 54, wherein sending the key to the client involves transmitting the key through a connection to a computer network.

64. (New) The method of claim 63, wherein the network connection is unencrypted.

65. (New) The method of claim 63, wherein the network connection is encrypted.

66. (New) The method of claim 63, wherein the computer network is the Internet.

67. (New) The method of claim 54, wherein the received authentication information includes a single-use code.

68. (New) The method of claim 54, wherein the received authentication information includes a event-based code.

69. (New) The method of claim 54, wherein the received authentication information includes biometric information.

a'

70. (New) A method implemented by a client for accessing secure information, said method comprising:

receiving an encrypted container from a third party, said encrypted container containing the secure information;

sending a key request including authentication information to an authentication server;

in response to sending the authentication information to the authentication server, receiving from a key server a key for decrypting the encrypted container; and

with the received key, decrypting the encrypted container to access the secure information.

71. (New) The method of claim 70, wherein said key request identifies the encrypted container.

72. (New) The method of claim 70, further comprising sending information to a storage server identifying the encrypted container, and wherein receiving the encrypted container the third party involves receiving the identified encrypted container from the storage server.

73. (New) The method of claim 70, wherein sending the key request and authentication information comprises, in response to sending the key request, receiving from the authentication server an authentication challenge and responding to the authentication challenge with the authentication information.

74. (New) The method of claim 70, further comprising, after decrypting the encrypted container, completely erasing the received key from all client memory.

75. (New) The method of claim 70, further comprising, after accessing the secure information, completely erasing the decrypted container and the secure information from all client memory.

76. (New) The method of claim 70, wherein the encrypted container contains a cryptrographic key.

77. (New) The method of claim 70, wherein the encrypted container contains a password.

78. (New) The method of claim 70, wherein receiving the key from the key server involves receiving the key through a connection to a computer network.

79. (New) The method of claim 78, wherein the network connection is unencrypted.

80. (New) The method of claim 78, wherein the network connection is encrypted.

81. (New) The method of claim 78, wherein the computer network is the Internet.

82. (New) The method of claim 70, further comprising generating a single-use code and wherein the authentication information comprises the single-use code.

83. (New) The method of claim 70, further comprising generating a event-based code and wherein the authentication information comprises the event-based code.

84. (New) The method of claim 70, further comprising generating biometric information and wherein the authentication information comprises the biometric information.

85. (New) The method of claim 70, further comprising using an authentication token to generate the authentication information.

86. (New) The method of claim 85, wherein the authentication token is a hardware device independent of the client.

87. (New) The method of claim 85, wherein the authentication token is connected to the client.

88. (New) The method of claim 85, wherein the authentication token is software running on the client.

89. (New) The method of claim 85, wherein the authentication token is software running on a processor independent of the client.

90. (New) The method of claim 70, wherein receiving the encrypted container involves receiving the encrypted container as an electronic communication over a network.